I have received a copy of the

Energy Systems Division
Computer Protection Plan

dated
January 2000

and I have read and understand
the information provided.

DRAFT ONE DO NOT CITE!!!

_____	_____
Print Name	**Badge No.**
_____	_____
Signature	**Date**

Return to John Anderson, ES, 362, Rm. E349

Internal
Document

Energy Systems Division
Computer Protection Plan

January 2000

Energy Systems Division
Argonne National Laboratory

Operated by The University of Chicago
under contract W-31-109-Eng-38, for the
United States Department of Energy

February 1997"

(http://www.anl.gov/CPP/cp_offl.htm)

will also serve as the Risk Assessment and Protection Plan for the Energy Systems Division (ES) as per the allowances in that document's introduction.

The following information is included as an addendum to describe specific services and staff available to the ES personnel and is included as a resource for ES division personnel.

Michael Vogt
ES Scientific Computing and Information Systems Manager
January 2000

General Computing Support

This document serves as an addendum to the Energy Systems Computer Protection Plan. It describes specifics about the division's systems, detailing anti-virus precautions, data protection (back up) procedures, and physical security.

The ES has a wide variety of research programs and supports a wide variety of platforms and computing needs. Investigators are encouraged to identify and use whatever operating systems and hardware best suit their research needs. Advice and support are available at the division level for most popular computer applications but specialized scientific software must be supported at the program level. The ES division has several specialized staff available for system support, with formal training in computer science and scientific applications use. These include Michael Vogt, Greg Krumdick, and John Anderson. ES also contracts with the Electronics and Computing Technologies (ECT) division to provide additional network and lab-wide system support. ECT staff available includes; Vito Berardi, Bob Krzebiot, and Peter Bertoncini.

ES Computer Support Staff

Computing Systems Manager	Computer Network Manager	Computer Protection Program Representative
Michael Vogt Bldg 362/B316 x7474 vogt@anl.gov	Greg Krumdick Bldg 362/B313 x3952 gkrumdick@anl.gov	John L. Anderson Bldg 362/E349 x6510 jlanderson@anl.gov

Network Computing Support

Vito Berardi	Bldg 362/C356	x8678	CSupport@anl.gov
Bob Krzebiot	Bldg 362/C356	x8678	CSupport@anl.gov
Pete Bertoncini	Bldg 222/A276	x4827	pjb@anl.gov
Tom Mackey	Bldg 221/D124	x9736	tkmackey@anl.gov

Computing Resources

ES has several computing facilities, one for the remote-accessed servers, one for computer support and repair and one for special purpose user workstations. The "Server Room" is Bldg 362/H-320. Entry is limited to designated computer support staff *only*. It houses six DELL Pentium systems running Microsoft Windows/NT [4.0]. These systems support remote dial-in access for authorized and authenticated ES staff, file and printer sharing, electronic mail systems, the ES Web server and groupware. The systems are managed both locally in the Server Room and remotely via authorized accounts.

ES maintains a computer support/repair lab in building 362/C356. This lab houses the computer support help desk. Requests for computer support can be made via e-mail to CSupport@anl.gov or by calling x8678 [supports voicemail]. Walk-in requests can also be made. There is also an analog phone line in this room for people to connect laptops to for dial-out access.

ES also maintains a computer workstation lab in the Center for Environmental Restoration System's (CERS) Spatial Analysis Laboratory (SAL). This lab has approximately twenty Windows/95/98/NT, MacOS, Sun SPARC10, InterGraph, and SGI Indigo/Indy UNIX workstations available with special purpose scientific applications (the cluster even runs a network operating system to allow parallel computing). These systems are maintained by the CERS staff and are available for divisional use. Special purpose computer graphics stations are available as well, with flatbed document scanners, photo slide scanners, film recorders, hi-quality color laser printers, digital cameras, video conferencing, and computer based data acquisition equipment. Wireless remote data collection is also available.

The spatial lab also maintains a suite of software development tools and has staff available to help with both advanced software system design and legacy software maintenance. Environments available include MS Visual BASIC, Visual Fortran, C/C++, Code Warrior, Java, assembly codes, microcontroller codes, expert systems, MATLAB, Mathematica, and a host of database systems including Paradox, Informix, Visual Analyst, and Access.

ES Computer Network

ANL is a MREN member and supports multiple connections to the Internet via OC3c ATM hardware. ANL has supported several paths to connect divisions to the site-wide network(s). In 1998 ES migrated from the Labwide FDDI shared 100 Mbps to ANL's Fast Ethernet Routing Hubnet. Deployed in 1993, ANL's Hubnet (hub network) backbone was established in a dual hub-and-spoke topology. The two hubs of the cable plant are in Buildings 221 and 308. At each hub of the cable plant is a Xyplex hub outfitted with fiber optic ethernet interfaces.

ES staff and projects occupy several buildings including 362, 369, 370, 371, 373, 376, and 200. The buildings with computers use the ANL network backbone(s) to maintain connections. ES's main building 362 physical connectivity to the Fast Ethernet Routing service is via multimode fiber optic cable in full duplex mode. All protocols, including IP Multicast and bridged protocols, are supported with the Fast Ethernet Routing service. This provided ES with its own dedicated 100 Mbps port.

Internally (each building is unique), ES maintains a 250+ node Ethernet network comprised of 10BaseT/100BaseTX/10BaseFL segments, legacy Ethernet 10Base2 (ThinNet), and even [limited] legacy LocalTalk mini-segments. All the segments are maintained through a RJ-45/Cat 5/ThinNet patch panel in the H-320 Server Room and are terminated in Cisco Catalyst 1900 and 2900 XL SmartSwitch, Cisco FastHub300, or SMC Tiger Ethernet Switches. Most Building 362 offices have (2) Cat 5 10BaseT connections (capable of dedicated 10 Mbps or 100 Mbps), but some offices still have only 10Base2 coax access (shared 10 Mbps).

Dial-in access to the ES server cluster is available [for travelers] via a 1-800 number (with a pool of two US Robotics 56K/x2 modems attached) and via a non-800 number (with a pool of two modems attached). The dial-in access is limited to 28K transfer speeds by external telco equipment. Standard Windows/NT authentication/challenge protects the dial-in access. Details will be provided to the ES user when the dial-in access in set up.

Computer Access Accounts

Computer accounts for the file servers [Appleshare-compatible, Windows Domain], groupware [Lotus Notes] servers, workstations [UNIX, IRIX, AIX], and e-mail are controlled solely through the division computer support staff. Requests for accounts must come from group leaders directly to support staff. Accounts for visitors are not allowed unless requested by ES division management. All expired accounts are locked or removed as requested by the owner's supervisor/group leader upon termination.

New employee/extended visitor accounts should be requested by staff from their center office. The request should be in writing/email message and include the person's name, supervisor, contact information, duration of appointment, and a short description of their role while in ES. Requests will be reviewed, set up, and activated. Changes to the accounts will require the staff member/visitor to present themselves to the ES administrators and show proper ANL badge to verify identity.

Computing System Network Security

Many ANL divisions encourage a shared "community" model for general ownership and general access to project files. The ES Windows/NT Windows/Applshare-compatible files are a good example of using this model to work effectively.

Authentication and access to the ES server cluster is provided through Windows/NT Domain Challenge.

All standard User Accounts are controlled through a Windows Primary Domain Controller with multiple Backup Domain Controllers. User passwords are filtered at the server level to force compliance with "strong password" strategies (>7 characters, with mixed upper/lower/special character sets). ES computer support encourages synchronized passwords for machine, domain, and screen dimmer use, as provided by any of the Windows password control panels. The domain servers challenge password and lockout accounts after a limited number (5-10) unsuccessful attempts. Administrator attention is required to reset this. Passwords are expired after 180 days, and tracked to prevent reuse of past passwords.

Approved security software is employed to regularly test the fitness of the authorized users' passwords and notify support administrators and staff of compromised (weak) passwords. The software used currently includes L0PHT Cracker 2.5.

ES also uses ISS Internet Security Software (current version ISS 6.0) as provided by ANL Computer Support personnel and license, to regularly scan each ES Windows/NT server and UNIX server. This software allows several levels of system interrogation and provides continued, updated, reports describing security weaknesses, possible exploitations, and recommended corrections.

Supplementing the ISS, passive intrusion detection software from Back Ice is run on several ES NT hosts to detect intrusion and to verify the active scanning from the ISS. Reports are generated and passed along to ES administrators.

Internet Access

Internet [World Wide Web] access is monitored on an occasional basis, and any questionable activity is corrected. Improper use of the ES computing systems, including Internet access, is handled as prescribed by the ANL Computer Protection Plan.

ES Maintains a World Wide Web server with a default home page tailored for staff at http://www.es.anl.gov. Information regarding division policy, directives, and project information are available there. Staff wishing to post pages/documents on the ES site need only include "WWW publishing" on their report/paper clearance forms to allow this. Live data access for projects can also be provided via the ES web site (databases available via Internet with web site interface). This includes Supervisory Control And Data Acquisition (SCADA) and expert systems applications as well. Interested staff can contact the web support via the ES home page. The web server and ES user Internet access is inspected using Web Trends reporting software. The information provided allows tailoring of the ES web site content and allows reporting of improper Internet access and use.

Electronic Mail

Until 1999, ES supported CE QuickMail for divisional use. QuickMail was available for MacOS and PC/Windows platforms, but the LAN version normally used was not Y2K compliant and QuickMail was phased out during 1999. ES adopted MS Exchange in 1999 as the default supported e-mail system. Exchange supports file sharing, facilities and resource scheduling, and Internet access to e-mail for travelers. The Exchange server supports IMAP4 and POP3 clients including QuickMail Pro, Outlook, Outlook Express, Netscape Mail, Eudora/Pro, and others.

ES staff monitor all DOE CIAC (Computer Incident Advisory Committee) broadcasts and take all required actions to protect ES internal systems

Physical Computer Security

The ES Server Room has complete physical security with a Cardkey access system for all authorized entry staff and a limited number [3] of hard keys maintained by the division management.

All staff offices and computing resource areas are locked and keys and entry controlled by appropriate key registration and protocol.

ES staff are also reminded that proper ANL-4 and ANL-8 material move orders are required to move equipment, including computers, between buildings and off site. If [computer] equipment is needed off site for more than 30 days, a shipping order is also required, as is a memo to ES division management defending the action.

Anti-Virus Computer Security

ES requires staff to run current versions of anti-virus software on their project machines. It is expected that the individual researchers will maintain version control and only notifications will be sent from the ES central computer support staff to the investigators. All computers on the ES network are expected to conform with Y2K compliance issues, with only MacOS 7 [or newer] or Windows95 [or 98 or NT or newer] operating systems being used. Symantic's Norton Anti-Virus 5 is the recommended anti-virus software for MacOS machines, and Command Antivirus 4.7 recommended for the Windows platforms. The ES divisional NT servers do NOT have anti-virus software running on the platforms themselves as this would pose a performance problem on servers. These servers are managed remotely from a separate Windows/NT platform that mounts each shared server drive and scans it separately, nightly. The MS Exchange e-mail server also runs the ExchangeScan software from Trend Micro to catch stray infections and Trojan horse [and other security problems] viruses at the server directly, before infected files reach the user machines. While this service lends an additional level of protection, it is expected that ES staff do not accept enclosures/attachments from unknown/unexpected sources.

Data Security

ANL policy indicates that the individual investigator(s) are responsible for protecting the data generated by their respective research projects. While this includes arranging and maintaining back-ups of computer files, ES computer support has made several options available to provide a uniform format for all ES project data.

Four of the ES Windows/NT servers have digital tape back-up drives for occasional archiving and data compatibility. The main back-ups are performed with a dedicated system recording on 70 gig DLTs. Incremental back-ups are performed for all servers nightly, with week's-end full back-ups performed Friday nights after hours. Each month, tape clusters are cycled out and stored in a secure vault in building 201 by ECT staff [Tom Mackey] contracted to maintain several divisional back-ups including ES. The ECT back-ups are meant to serve as "disaster recovery." ES also have two CD-W/ROM drives for CD-ROM archiving of project data. Arrangements can be made for this service through divisional computer support staff listed above.

Individual staff computers can also be backed-up over the ES intranet. Arrangements can be made through support staff. This service is available for MacOS machines or Windows/95/98/NT machines, and can record on a variety of media including DDS3 and DLT.

Data Encryption and Secure Software

To comply with the need for secure network access, telnet and ftp are being replaced with secure shell compliant client software. SecureCRT has been recommended for use at ANL and at most local universities including University of Chicago and Illinois Institute of Technology. The SecureCRT software can be downloaded through ECT Account Services by e-mailing ECT and requesting registration as a user.

Data encryption applications can be suggested and provided upon request.

ES Y2K Preparedness

ES has had a Y2K Preparedness Plan in effect throughout 1999 and all machines were either verified to be Y2K compliant, were updated to meet Y2K compliance, or were removed from the ES network. Y2K compliance was defined by ANL Computer Protection Group and a table detailing the ES system testing and completion is available in a separate ESD Y2K Protection Plan document.